PLEASE CLICK ON THE COUNTY OF LOS ANGELES SEAL
TO RETURN TO THIS PAGE

CLICK HERE FOR THE INFORMATION SYSTEMS ADVISORY BODY'S REPORT DATED NOVEMBER 8, 2016

Information Systems Advisory Body
County of Los Angeles

November 8, 2016

TO: Supervisor Hilda L. Solis, Chair
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: Ali Farahani
ISAB Director

SUBJECT: **Developing a Countywide Digital Evidence Management Strategy (Item No. 2, Agenda of July 12, 2016)**

On July 12, 2016, your Board directed "the Information Systems Advisory Body in collaboration with the Executive Director of the Countywide Criminal Justice Coordinating Committee, District Attorney, Public Defender, Alternate Public Defender, County Counsel, Chief Executive Officer, and other public safety and justice partners to develop an implementation strategy for a Countywide Digital Evidence Management System (**DEMS**) based on open industry standards and report back to the Board of Supervisors in writing in 120 days."

The Information Systems Advisory Body (ISAB) established a Committee that was comprised of representatives from the following agencies:

- Sheriff's Department
- District Attorney's Office
- Public Defender
- Alternate Public Defender
- Probation Department
- Los Angeles Superior Court
- Internal Services Department
- County Counsel
- Chief Executive Office
- Office of the CIO
- Countywide Criminal Justice Coordinating Committee
- Office of Inspector General
- Long Beach Police Department

The first meeting of the Committee was held on July 28th, 2016 and the Committee continued to meet bi-weekly between August 11 and October 6, 2016.

FINDINGS AND RECOMMENDATIONS:

The emergence of digital content as a common form of evidence in criminal cases has created a new business challenge for the criminal justice agencies in Los Angeles County. The growing volume of digital data as potential evidence, the variety of digital content types, the need to protect the authenticity and integrity of such data during the lifecycle of a criminal case, and the requirement for discovery and sharing of potential evidence and collaboration among justice agencies all demand an enterprise approach and the development of an integrated solution.

The Committee reviewed key criminal justice business process areas that involve the capture and management of digital content and technology areas that form both the application layers and the foundation and infrastructure for solutions to manage digital content in compliance with statutory and regulatory mandates.

The County of Los Angeles needs to develop a common infrastructure and an enterprise platform for digital evidence management to fully support the lifecycle of "digital" evidence for justice agency stakeholders within Los Angeles County, each of which has unique business requirements for the capture, storage, management, protection, and sharing of digital content that could become digital evidence. It is important to note that each stakeholder in the criminal justice system has unique business requirements for staff access, application functionality, software toolset to work with digital content, and management of digital content.

The system architecture of a Countywide digital evidence management system must meet multiple layers of business, functional, and technical requirements. The system must support a multi-modal integration framework based on open industry standards. These include methods for ingestion of content into the system and secure linkage and integration with departmental content and case management systems. The system must also comply with industry standards for protecting the authenticity of digital content using digital signatures. Protection of privacy, confidentiality requirements, user role-based access control, and audit logs are among other requirements for a reliable, trusted, and secure digital evidence management system. The Committee developed Figure 1 to depict a high-level architectural view of the scope and components of the system.

The lifecycle of digital evidence starts as content recorded by an electronic device. An electronic device captures and stores data on magnetic, optical, or solid-state drive (SSD) storage media. These data are stored in what is known as a "data file". All digital content is stored as a file. Files have different formats depending on the type of data they encode (text, video, audio, medical imagery). Files can be in human or machine readable formats. A digital evidence management system stores, manages, and protects all data regardless of file content or format. The Committee emphasized the need to develop a digital evidence management system architecture that can manage all types and forms of digital evidence in line with the business requirements of all the stakeholders in the criminal justice system. Digital evidence could be generated or captured by Body Worn Cameras (BWC) or Closed-circuit television (CCTV), Crime Scene video and images, 911 calls or other audio recordings, video that is captured by the general public, private businesses or the media, documentation that is scanned and converted to digital files, digital content from computers, cellular phones, and other electronic devices.

County of Los Angeles Digital Evidence Management System

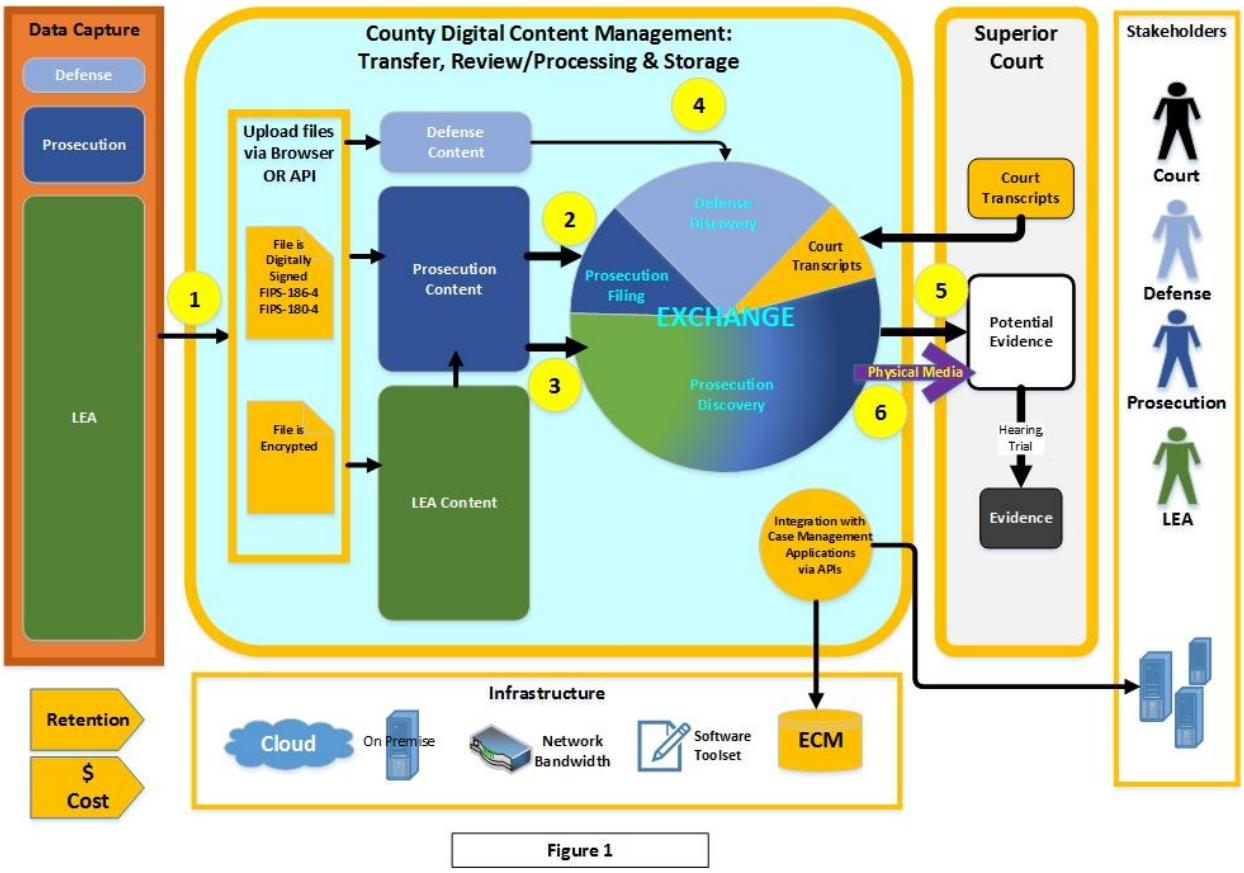

Figure 1

Digital evidence management systems not only serve as reliable repositories of content but also must meet the application functionality requirements of each of the stakeholders in the criminal justice system. These include digital content metadata management, search, annotation, creating derivative content from original, redaction, and transcription. The system must also support granular role-based content security and access control. Chain of Custody and cyber security requirements mandate that the system support audit logs for all access.

Enterprise digital evidence management systems serve a dual role: they allow each of the stakeholders in the criminal justice system to have a "private repository" to manage content that they own and at the same time facilitate "discovery" and the "moderated" transfer of content from one entity to another.

It is also important to note that any Countywide digital evidence management system must function in a heterogeneous systems environment. Los Angeles County criminal justice system stakeholders have major investments in a variety of technologies and it is a mandatory requirement that any DEMS system must support open industry standards for interoperability and integration with all stakeholder systems.

The Committee acknowledged that departments already have one or more line-of-business case and content management systems that are used to manage work, documents, and cases. The development of a Countywide digital evidence management system needs to consider how such a system could be integrated with existing departmental Enterprise Content Management (ECM) and Case Management Systems, and future BWC video collection application software.

There are several statutory and regulatory requirements that must be included in the design and implementation of a digital evidence management system. These requirements are put in place to protect the integrity of the system and its content and hence ensure trust and confidence in the system. The Committee reviewed the most relevant statutory and regulatory requirements as well as industry standards that should govern the implementation of a Countywide system.

Currently, the Superior Court does not support the electronic transmission of digital content as potential evidence. The Judicial Branch's Information Technology Advisory Committee will be considering "Digital Evidence Management" as an annual agenda topic for 2017. If it officially makes it on the list a "workstream" will be formed to establish court standards and modernize Court rules and legislation as they relate to digital evidence management. County's DEMS strategy must accommodate an eventual implementation of electronic submission of digital evidence by the court. Another important consideration is that the transmission of electronic evidence to the Superior Court must also be acceptable by the Court of Appeal.

The storage and management of large digital files within a digital evidence management system requires further research and evaluation of how the implementation and deployment of such a system and the consequential increase in bandwidth requirements could impact County's data network infrastructure.

RECOMMENDATION #1: County establish a Digital Evidence Management System Steering Committee to provide leadership and oversight in the development and implementation of a system to meet the business requirements of all criminal justice agencies in the County of Los Angeles.

RECOMMENDATION #2: County initiate a new project to develop and document the business requirements for a Countywide Digital Evidence Management System. We further recommend that ISAB engage the service of an expert consultant to work with County criminal justice agencies and partners to assist in gathering and developing the requirements to release an open solicitation for an information technology solution for digital evidence management by January 31, 2018.

RECOMMENDATION #3: A fiscal committee be created for developing comprehensive cost estimates and identify funding requirements for the development of a Countywide Digital Evidence Management System.

RECOMMENDATION #4: Internal Services Department to develop a plan to take adequate measures to ensure County's enterprise network infrastructure can accommodate the bandwidth requirements of County departments deploying systems that manage digital evidence.

HIGH-LEVEL REQUIREMENTS AND ANALYSIS:

The Committee examined the business process requirements of the four classes of stakeholders (law enforcement, prosecution, defense, and judicial) in the criminal justice system in the following seven categories:

1. Department's particular business requirements for digital evidence management
2. The types (and sources) of digital evidence for each department
3. How each department is currently managing digital evidence
4. The volume (number and size of digital files) of digital evidence currently managed by each department

5. How each department manages "digital" evidence compared to "evidence management" in general
6. Applicable "record retention" requirements for digital evidence for each department
7. Statutory requirements for sharing and access to digital evidence that each department has to comply with

The Departments' responses were consistent, differing only in breadth, emphasis and detail. No one department's requirement conflicted with another's requirement. The individual responses are collated and are summarized below. The detailed responses are included as Attachment A.

- *Evidence Preservation; Authentication and Admissibility:* Contributors emphasized the importance of an expedient and flexible process for submitting content of all types while preserving its integrity and admissibility.

- *Evidence Review, Redaction and Analysis:* Contributors called for baseline performance and functionality consistent with standard digital forensics and e-discovery products, to include searching, viewing, redacting, excerpting, and annotating digital evidence within a collaborative environment.

- *Presentation:* Contributors emphasized the need to present evidence in a variety of settings, with and without network access. Attorneys emphasized the need for unrestricted access to qualified custodians and engineers for advice and testimony.

- *Users and User Experience:* Stakeholders called for a comprehensive, adaptive interface, compatible across platforms, to accommodate the broad spectrum of end-user needs and competencies. They highlighted the importance of swift user onboarding.

- *Scope:* Contributors stressed the importance of flexibility to accommodate unanticipated requirements and out-of-band storage.

- *Auditing and Compliance:* Stakeholders spotlighted the importance of detailed logging of user activity, and the necessity for immediate and unrestricted access by authorized information security personnel to native log files and other information relevant to the detection and investigation of information security incidents.

- *Information Sharing and Interoperability:* Stakeholders emphasized the need for fluid information sharing and efficient work flow amongst departments, their business associates and outside agencies, protected by strong safeguards to detect and prevent unauthorized or unintended exposure. They highlighted the requirements of open-standards, interoperability with industry standard digital forensics and e-discovery tools.

- *Security:* Throughout, contributors emphasized the necessity of data integrity, availability and confidentiality. They called for compliance with best practices including encryption in transit and at rest, implementation of CIS (Critical Information Security) controls, and comprehensive forensic readiness. Particular emphasis was placed on the necessity for swift reporting of information security incidents to, and full cooperation with, County law enforcement.

1. What are your department's business requirements for digital evidence management?

   a. Evidence Preservation; Authentication and Admissibility

1. Material shall be stored in original format and all metadata shall be retained. Files must not be split or converted in any way.
2. Submission process shall be swift and shall not create bottlenecks that tie up equipment or stymie personnel.
3. Submission process shall be flexible to accommodate various sources of evidence.
4. There shall be a simple, open source, repeatable means for proving that the file uploaded/downloaded was the file stored/requested (e.g. cryptographic hash computed and stored contemporaneous with upload).
5. Chain of custody shall be recorded and maintained, based upon strong authentication.

b. Evidence review, redaction and analysis
   1. System must facilitate redaction, including advanced "smart" redaction for moving and still images, while retaining a pristine original.
   2. System must provide still and moving image analysis and enhancement functionality.
   3. System shall allow annotation and collaboration without modification of original.
   4. System shall provide search and selection functions that shall include: Index, keyword and RegEx (Regular Expression language) search, bookmarking and extraction. All search and selection functions shall be scriptable. Performance shall be consistent with industry norms.
   5. System shall accommodate multiple displays of varying resolution.
   6. Users must be able to work offline.

c. Presentation
   1. Users need to present evidence to colleagues, witnesses, experts and others, in a variety of settings.
   2. In court, lawyers need the ability to present evidence with or without reliance on courtroom facilities such as audiovisual systems and network connections.
   3. Investigations and court proceedings are fluid, fast paced and unpredictable. Trial teams must be able to react to court rulings and evolving facts without system-induced friction (e.g. redact on the fly).
   4. Vendor shall provide consultation during trial preparation and live testimony in court. A qualified custodian of records must be readily available for consultation regarding foundation and authentication issues. If trial deputy deems it prudent or necessary, qualified custodian and qualified engineer must be based in Los Angeles or an adjoining county, must be amenable to service of process, and available to testify without fee, providing expert witness testimony of their DEMS technology, when requested by County.
   5. Users shall be able to present evidence offline.

d. Users and User Experience
   1. The full feature set shall be available on all platforms (minimally Windows, OS X and iOS) and shall be fully accessible using any common browser (minimally Chrome, Explorer and Safari). Applications shall be fully compliant with each platform's human interface guidelines.
   2. System must offer a dashboard style interface capable of managing all digital evidence, and customizable based on role and individual user preferences.

3. System must accommodate varying levels of user skill and sophistication, with a gentle learning curve for basic functions.
4. The authentication scheme shall allow for access by law clerks and outside experts, without a lengthy approval process.

e. Scope
   1. The system and related policies shall provide flexibility to accommodate unanticipated requirements and out-of-band storage.

f. Auditing and Compliance
   1. System shall record, maintain and retain a detailed audit trail of all user activity, attempted or completed.
   2. Vendor shall provide immediate and unrestricted access by authorized information security personnel to native log files and other information relevant to the detection and investigation of information security incidents.

g. Information sharing and interoperability
   1. The system shall provide the tools necessary for information sharing and work flow amongst all the stake holders, their business associates and outside agencies. For example, the system must allow police agencies to exchange BWC and other evidence, facilitate electronic submission from third parties to police, from police to prosecutor, from prosecutor to defense, from attorneys to experts and to the court.
   2. The system shall organize all digital evidence by case and allow synonymous naming to accommodate stakeholders' case numbering conventions.
   3. All information, including original material, metadata and work product, shall be portable without additional cost, to assure continuity and independence. Upon the completion or termination of Agreement, Vendor shall submit to the County at no cost, all data, in County designated and requested formats and media, including with all corresponding metadata.
   4. System shall facilitate compliance with court rules regarding admission of audiovisual exhibits, court orders for the duplication of evidence and disposal.
   5. System shall be compatible with industry standard digital forensics and e-discovery tools (e.g. EnCase, FTK, IEF, Nuix, e-discovery platforms).
   6. System shall convert proprietary file format to open-standard format, while preserving intact the original file.
   7. System shall provide strong safeguards to prevent accidental publication, i.e.: mistakenly sending the wrong content to the wrong person.
   8. System shall provide strong safeguards to detect and prevent deliberate or inadvertent exfiltration, modification or destruction.

h. Security
   1. All digital evidence and other customer data shall be stored in a secured environment, free from intentional and unintentional access, contamination, modification and destruction.
   2. System shall provide Reasonable Security, at a minimum compliance with the CIS top 20 critical information security controls.
   3. All digital evidence and other customer data shall be encrypted at rest and in transit.
   4. Vendor shall notify County within four (4) hours of detecting an information security incident. he term "information security incident" includes any actual or suspected adverse event, attempted or completed, including *inter alia*, unauthorized

account access; unauthorized data exposure, disclosure, modification or destruction; disruption or denial of availability; compromise of network or systems used by the County or on which County data are stored.

5. All system and network components must be configured to record and preserve evidence in order to facilitate the discovery, investigation, and possible prosecution of unauthorized access, whether attempted or completed.
6. Vendor shall cooperate fully with law enforcement in the investigation of information security incidents, including determination of incident scope. Vendor shall not demand legal process except when required by law.

2. What are the types (and sources) of digital evidence for your department?

a. Sources:
    1. Incident created (BWC Video, crime scene photos, incident reports, etc.)
    2. Investigator created
    3. Investigator/DA captured/retrieved
    4. Produced by legal process, consent
    5. Provided by outside agencies, crime victims, defense attorneys, witnesses
b. Types
    1. Reports and documents (doc, pdf, xls, txt, etc.)
    2. Still images
    3. Moving images (many formats, surveillance, BWC, dash cam, cell phone)
    4. Audio recordings (many formats)
    5. Forensic (cell phone and other images, log files, etc.)
    6. Binary images, E01's
    7. Proprietary/specific formats (eg: evtx, pst)
    8. CAD files
    9. Additional types emerge regularly
c. Special issues
    1. Child Pornography (CP)
    2. Malware
    3. Forensic images (file sizes > 1 TeraByte)
    4. Heterogeneous file formats, malformed, fragmented data
    5. Encrypted
    6. Compressed

3. How is your department currently managing digital evidence?

a. Mostly on physical media (DVD, flash drives, etc.)
b. Internal file shares
c. Some BWC video from LAPD and other agencies on evidence.com (cloud-based)
d. Some transferred by other means (secure FTP, other file sharing)
e. High Tech Crimes evidence managed by DA's Bureau of Investigation

4. What are the volumes?

a. Because much of the evidence is managed by individual attorneys on physical media, it is difficult to estimate volumes.

b. However, some information is available based on the LAPD Pilot of evidence.com. For 4 pilot divisions, approximately 1 year, there is 2 TeraByte of video data referred to the District Attorney.
c. Also, the DA Bureau of Investigation Sound Lab, which handles digital recordings processes and stores 3.5 – 4.0 TeraByte annually.

5. How does "digital" evidence management tie to "evidence management" in general?

a. Digital evidence management is ideally a subset of evidence management in general. However, the nature of it is such that it lends itself to better storing and tracking the information.
b. Both digital and material evidence are subject to the same chain of custody and discovery protocols.
c. The Bureau of Investigation currently separates digital evidence management from material evidence but is proposing to upgrade material evidence management to an electronic evidence collection and management system.

6. What are the applicable "retention" requirements for your digital evidence?

a. 5 years for misdemeanor case files and evidence
b. 25 years for felony case files and evidence EXCEPT as provided below:
c. Indefinite for life and capital case files and evidence
d. 5 years for declined cases, after declined for further action

7. What are the statutory requirements for access to digital evidence that your department has to comply with?

a. Criminal Justice Information Services (CJIS) Compliance (28 CFR Part 23)
b. Standards set by International Association for Property and Evidence, Inc. (IAPE)
c. Cal. Pen. Code sec. 1546 et seq (CalECPA)
d. California Evidence Code
e. Federal Rules of Evidence
f. Title III
g. Adam Walsh Act (Child Pornography)
h. Special situations – trade secrets, protective orders, special privacy orders (census data, federal tax returns), Protected Health Information (PHI), Department of Children and Family Services (DCFS), juvenile offender records
i. Highly sensitive documents: proffers, plea negotiations, grand jury materials
j. Cal. Civ. Code § 1798.81.5(b) (Data breach reporting)
k. County Code Requirements, including BOS 6.100 et. seq.

c: Chief Executive Office
Executive Office of the Board of Supervisors
Countywide Criminal Justice Coordinating Committee
Office of the CIO
County Counsel
District Attorney
Sheriff
Public Defender
Alternate Public Defender
Probation
Los Angeles Superior Court
Office of Inspector General
Internal Service Department

ATTACHMENT A

A. Sheriff's Department

1. [incorporated above]

2. What are the types (and sources) of digital evidence for your department?
    a. All evidence that is currently, or can be converted to, digital evidence, including but not limited to:
        1. BWC video
        2. Audio files (i.e., 911 calls)
        3. Photo stills (crime scene)
        4. Citizen uploaded Digital Evidence (DE)
        5. Search warrant obtained DE (i.e, mirroring a Smart Device)
    b. Currently, all DE submitted to the CA/DA are provided on hard media and hand delivered
    c. There are many current LASD systems that have digital files (e.g., SECDA, Mideo, CCTV), but only DE identified as evidence that's transferred to other law enforcement and justice agencies will utilize DEMS for an electronic transfer
    d. LASD's long-term goal is to submit/file a case to the DA or CA electronically, thereby eliminating or greatly reducing physical delivery

3. How is your department currently managing digital evidence?
    a. Digital media inventoried in PRELIMS as hard media (e.g., DVD, SD card)
    b. Sent to DA on digital media devices (DVD, Smartcard, Flash Drive, etc.), or in hardcopy (photographs, reports, and other pertinent documentation)
    c. When required, photo or video analysis or enhancement is performed by high-tech task force or crime analysts

4. What are the volumes?
    LASD conservatively estimates between 6 and 11 petabytes of DE upon full BWC deployment, with an increase for cases (e.g., murder, rape) where DE is retained indefinitely. Upon LASD's Phase I deployment, more accurate estimates will be provided

5. How does "digital" evidence management tie to "evidence management" in general?
    LASD's 'evidence management' system is PRELIMS, where that system's focus is physical evidence. Presently, digital evidence resides on a media device (e.g., DVD, SD card) and it's that device that's inventoried in PRELIMS (where its movement is tracked). As more and more evidence is collected in digital format, the process will most likely change, where DEMS takes precedence

6. What are the applicable "retention" requirements for your digital evidence?
    a. 2 years (infractions, non-criminal and other business records)
    b. 9 years (misdemeanors and felonies)
    c. Indefinite

7. What are the statutory requirements for access to digital evidence that your department has to

comply with?

a. CJIS Compliant and/or current cyber security best practices
b. California Assembly Bill 69
c. California Evidence Code Compliance
d. Federal Rules of Evidence Compliance
e. County Code Requirements
f. LASD MPP Requirements
g. Justice Information Sharing Initiative Compliance

B. District Attorney

The District Attorney's Office manages digital evidence in several key areas: Prosecution, Investigation, and Cyber Investigation Response.

DA – Retention Periods

Title	*Description*	*Retention Period*	*Authority Citation*
Bad Check Program Files	Includes: Accounting documents, payment schedules, police reports, contract documents, bank statements, affidavits, correspondence, and related records.	5 years after case closed	
Criminal Case Declined Files	Contains cases investigated and formally declined for further action by the office. Includes: Police or Sheriff's reports, witnesses' statements, evidence gathered, investigation materials, and related records	5 years after case declined for further action	
Criminal Case Files-Felonies	Includes: Police or Sheriff's reports, motions, affidavits, witnesses' statements, criminal records of defendants, working papers and notes developed by Prosecuting Attorney used in preparing the case for prosecution and other supporting documents relative to case.	25 years after case closed or permanent, depending on type of case	California Attorneys for Criminal Justice (CACJ) v County of Los Angeles-BC161572
Criminal Case	Includes: Police or Sheriff's reports,	5 years after case	California Attorneys

Files-Misdemeanors	motions, affidavits, witnesses' statements, criminal records of defendants, working papers and notes developed by Prosecuting Attorney used in preparing the case for prosecution and other supporting documents relative to case.	closed	for Criminal Justice (CACJ) v County of Los Angeles-BC161572
Open Investigation Case Files	Contains open cases under investigation by the office. Includes: Police or Sheriff's reports, witnesses' statements, evidence gathered, investigation materials, and related records	Review annually for continued retention or move to Criminal Case Declined Files	
Victim Assistant Case Files	Includes: Victim profiles, witness testimony, investigation materials, and related records.	5 years after case closed	

C. Public Defender and Alternate Public Defender

1. [incorporated above]

2) What are the types (and sources) of digital evidence for your department?
   a) The PD attorneys and support staff often request USB Flash and Hard drives for video and documents. Video files are increasing especially with the body cam worn videos.
   b) We anticipate that all PD Investigators and Attorneys will be obtaining videos via PD provided media from all justice agencies such as LEA's and DA's.
   c) Types of files can be:
      i) PDF
      ii) MS Office type documents
      iii) Video – all formats (including Proprietary formats)
      iv) Audio – all formats
      v) Photos – all formats

3) How is your department currently managing digital evidence?
   The Public Defender currently does not have an adequate method to store digital evidence. Currently, IT is currently providing external hard drives and USB Flash Drives to attorneys and paralegals. We also provide Box.com Cloud storage as a means to upload discovery and videos from LEA's and from the DA's.

4) What are the volumes?
   We currently receive most videos from the DA, Law Enforcement Agencies, and other justice partners. However, the Public Defender must provide their own media such as Flash or Hard drives to obtain the videos. The size of the media has increased to 1 – 3 TB requests due to the

increase of video uploads as opposed to documents.

5) How does "digital" evidence management tie to "evidence management" in general?
   Paper evidence and digital evidence will ultimately need to be archived. Most evidence are scanned into PDARTS and digital evidence are archived at our warehouse as non-scannable items. Currently, there is no marriage of the two types of evidence as whole.

6) What are the applicable "retention" requirements for your digital evidence?
   The statuary retention requirements is currently for the life of our client.

7) What are the statutory requirements for access to digital evidence that your department has to comply with?
   a) CJIS Compliance (28 CFR Part 23)
   b) Standards set by International Association for Property and Evidence, Inc. (IAPE)
   c) Cal. Pen. Code sec. 1546 et seq (CalECPA)
   d) California Evidence Code
   e) Federal Rules of Evidence
   f) Title III
   g) Adam Walsh Act (Child Pornography)
   h) Specific privacy issues – trade secrets, protective orders, special privacy orders (census data, federal tax returns), PHI, DCFS, juvenile offender records
   i) Cal. Civ. Code § 1798.81.5(b) (Data breach reporting)
   j) CA Bar Rules of Professional Responsibility (duties of confidentiality, loyalty and candor)
   k) County Code Requirements, including BOS 6.100 et. seq.
   l) California BAR mandate to keep case files and video indefinitely for the life of the client.

D. Probation Department

1. [incorporated above].

2) What are the types (and sources) of digital evidence for your department?
   a) Sources:
      i) Investigator created
      ii) Produced by legal process, consent
      iii) Provided by outside agencies
   b) Types:
      i) CCTV video footage
      ii) Audio Recording
      iii) PDF documents
      iv) Still Photos
      v) Court Reports, Digital Image
      vi) Email

3) How is your department currently managing digital evidence?
   a) ISD eCloud service for documents
   b) O365 for emails
   c) CCTV footage are store in local servers

d) DVDs
e) USBs
f) External hard drive

4) What are the volumes?
a) CCTV video footage – 1,176 PB (1,176 TB)
b) Audio Recording – 800 TB
c) Documents and Still Photos – 10 TB
d) Court reports (pdf) and digital image – 3 TB
e) Email – 12 TB

5) How does "digital" evidence management tie to "evidence management" in general?
Probation's PEDMS (Probation Enterprise Document Management System) store all Court Reports and related digital images. Presently, digital evidence is shared and resided on a media device (e.g., DVD, SD card, external hard drive)

6) What are the applicable "retention" requirements for your digital evidence?
a) 1 year (365 days) – CCTV video footage from Camps and Halls
b) Physical files – 5 years post jurisdiction termination
c) Civil Litigation purposes – 7 years
d) Email – 5 years with a litigation hold of indefinite

7) What are the statutory requirements for access to digital evidence that your department has to comply with?
a) CJIS Compliance
b) California Evidence Code Compliance
c) Federal Rule of Evidence Compliance
d) County Code Requirements
e) California Assembly Bill 69

E. Superior Court

1. [incorporated above].

2.What are the types (and sources) of digital evidence for your department?
Typically, the court receives audio recordings, video recordings, and digital photographs as evidence, received via CDs, DVDs, or flash drives generally.

3. How is your department currently managing digital evidence?
Currently, digital evidence is stored on CDs, DVDs or flash drives (on rare occasions: VHS and cassette tapes) prior to being submitted to the court as evidence. California Rule of Court 2.1040 requires a transcript to be submitted along with an electronic recording presented as evidence.

4. What are the volumes?
Unknown at this time for the court.

5. How does “digital” evidence management tie to “evidence management” in general?
   The court's chain of custody and related documentation are imperative once evidence is introduced in a court proceeding. Exhibits must have an evidence tag affixed to it for identification purposes (how digital evidence would be tagged should be a key discussion point). Controlled access to evidence, digital or otherwise, is required. The court needs to maintain documentation regarding who viewed the exhibits and when, and whether or not the exhibits were reproduced. In addition, evidence introduced as a trial court exhibit must be disposed of when the retention requirements have been met, as set forth in Penal Code 1417 and Code of Civil Procedure 1952.

6. What are the applicable “retention” requirements for your digital evidence?
   For criminal/juvenile exhibits, the retention requirements are set forth in Penal Code 1417. For civil exhibits, the retention requirements are set forth in Code of Civil Procedure 1952.

7. What are the statutory requirements for access to digital evidence that your department has to comply with?
   The chain of custody of evidence must be retained at all times, including documentation of who accessed the evidence and when. In addition, the court must allow access to evidence for viewing and/or reproduction purposes after application and order has been made (exceptions apply).